Martti Lehto, Jyväskylän yliopisto
29.4.2022

Eduskunnan hallintovaliokunta

Asia: Ajankohtaisselonteko turvallisuusympäristön muutoksesta, VNS 1/2022 vp

1. DIGITAALINEN TOIMINTAYMPÄRISTÖ MURROKSESSA

Selonteko toteaa oikein, että ”Venäjän käynnistämä sota vaarantaa koko Euroopan turvallisuuden ja vakauden.” Tämä vaarantaa koko digitaalisen maailman toiminnan, jossa kansalaiset, yritykset ja julkiset toimijat muodostavat verkottuneen ja keskinäisriippuvan toimintaympäristön.

Modernin yhteiskunnan toiminta perustuu kansallisen kriittisten infrastruktuurin useiden eri osien yhteistoimintaan. Niiden keskinäinen toimintakyky riippuu yhä enemmän kyberturvallisista ja korkean käyttövarmuuden omaavista sähköjärjestelmistä ja tiedonsiirtoverkostoista sekä muista luotettavista ja tietosisällöltään eheistä hallinnon ja kansalaisten palveluista.

2. VENÄJÄN NÄKEMYS KYBERSODANKÄYNNISTÄ

2.1 RuNet

Vuonna 2017 Venäjän hallitus sanoi, että vuoteen 2020 mennessä maa aikoo pitää 95 prosenttia nettiliikenteestä Venäjän rajojen sisällä. Vuonna 2018 Venäjä esitteli päivitetyn *Kansallisen digitalousohjelman*, jonka mukaan Venäjän Internet-palveluntarjoajien tulee taata toiminnan jatkuvuus myös tilanteessa, jossa ulkomainen taho yrittää eristää Venäjän kansainvälisestä verkosta.

Syksyllä 2019 hyväksyttiin laki suvereenista Runetista, joka on suunniteltu suojaamaan Venäjän Internet-segmenttiä ulkopuolisilta uhilta. Lain mukaan kaikkien maan operaattorien verkkoihin on asennettava erityislaitteet, joiden kautta Roskomnadzor pystyy tarvittaessa hallitsemaan liikenteen reititystä. Laki laitteiden asentamisesta tuli voimaan vuonna 2020. Roskomnadzor voi katkaista verkkoliikenteen milloin ja miten haluaa. Se voi katkaista yhteydet kaikkiin ulkomaisiin palvelimiin, tai rajata katkaisun suomalaisiin IP-osoitteisiin tai .fi-päätteisille verkkosivustoille.

Venäjä testasi RuNetin irrottamista loppuvuodesta 2019, sanoen sen onnistuneet. Tätä ei ole voitu varmentaa.

2.2 Venäläiset verkkopalvelut

Oman tietoliikenneverkon rakentamisen ohella Venäjällä on rakennettu omia sosiaalisen median palveluita, jotka ovat vastaavia länsimaisten palveluiden kanssa. Venäjällä on rajoitettu kansalaisten pääsyä läntisiin Internet-palveluihin.

2.3 Venäjän Uuden sukupolven sodankäynti

Latvialaisen tutkijan Jānis Bērziņšin mukaan Venäjä on siirtymässä kohti *Uuden sukupolven sodankäyntiä*. Siinä on länsimaiden käyttämän hybridisodankäynnin elementtejä, mutta kineettisen voiman käyttö ei ole keskiössä tai sen käyttö ei aina ole edes välttämätöntä. Hänen mukaansa uuden sukupolven sodankäynti tuottaa seuraavanlaisen muutoksen:

1. Suorasta tuhoamisesta suoraan vaikuttamiseen.
2. Vastapuolen tuhoamisesta sen sisäiseen mädättämiseen.
3. Asein ja teknologian avulla käytävästä sodasta kulttuurisotaan.
4. Tavanomaisilla joukoista käydystä sodasta erikoisjoukkoihin ja yksityisiin sotilasalihankintayrityksiin.
5. Perinteisestä kolmiulotteisesta taistelukentästä info-/psykologiseen sodankäyntiin.
6. Suorasta yhteenotosta sotaan ilman kontaktia.
7. Pinnallisesta ja ositetusta sodasta totaaliseen sotaan.
8. Fyysisestä toimintaympäristöstä sotaan ihmisen tietoisuudessa sekä kyberavaruudessa.
9. Symmetrisestä sodasta asymmetriseen sotaan yhdistämällä poliittisia, taloudellisia, teknologisia sekä informaatio-, ja ympäristökampanjoita.
10. Rajatun mittaisesta sodasta pysyvään sotaan kansakunnan luonnollisena olosuhteena.

Ukrainan sodassa Venäjä käyttää edelleen perinteisiä keinoja, mutta pyrkii myös vahvistamaan siirtymää Uuden sukupolven sodankäyntiin. Venäjä tulee käyttämään tämän konseptin keinovalikoimaa Suomea vastaan käynnissä olevan NATO-prosessin aikana.

2. POLIITTINEN ULOTTUVUUS

2.1 Kyberpolitiikka ja -diplomatia

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne (engl. Cyber Politics). Kybertoimintaympäristö on jatkuvassa muutoksen tilassa, ja tätä kehitystä pyritään poliittisin keinoin ohjaamaan. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla

kansainvälisillä foorumeilla ja järjestöissä kuten ETYJ:ssä, EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa.

Diplomaattinen valta on neuvotteluissa ja sopimuksissa, joiden tarkoituksena on sitoa osapuolia yhteisesti sovittuihin toimiin. Kyberdiplomatiassa tarkoituksena on käsitellä alan kansainvälistä oikeutta ja normeja, kyberturvallisuutta ja muita toimia, joilla lisätään luottamusta. Keskinäisen yhteisymmärryksen ja yhteisten pelisääntöjen avulla voidaan vähentää erilaisten konfliktien uhkaa.

EU on jo muutamien vuosien ajan kiinnittänyt huomiota kyberdiplomatiaan. EU:n neuvosto päätti 2017 kehittää kyberdiplomatiaan välineistön, joka on EU:n yhteinen diplomaattinen vastaus haitallisiin kybertoimiin. Vuonna 2018 EU julkaisi päätelmät haitallisista kybertoimista. Päätelmissä korostui kybertoimintaympäristön vapaus, vakaus, turvallisuus, avoimuus ja globaalius. EU:n neuvosto vahvisti kehyksen vuonna 2019, jonka avulla EU voi määrätä kohdennettuja rajoittavia toimenpiteitä, joilla estetään ja vastataan kyberhyökkäyksiin, jotka muodostavat uhkan EU:lle tai sen jäsenvaltiolle. Myös kyberhyökkäykseen osallistuneet kolmannet maat tai kansainväliset järjestöt voivat olla toimenpiteiden kohteena, jos se katsotaan tarpeelliseksi ulko- ja turvallisuuspolitiikan tavoitteiden saavuttamiseksi.

EU käytti tätä välineistöä ensimmäistä kertaa heinäkuussa 2020, kun neuvosto päätti määrätä rajoittavia toimenpiteitä useista kyberhyökkäyksistä vastuussa olevia tai niihin osallistuneita kuutta henkilöä (Kiina, Venäjä) ja kolmea yhteisöä (Kiina, Pohjois-Korea, Venäjä) vastaan.

Kyberturvallisuudessa valtioiden välisen luottamuksen lisääminen on keskeinen kysymys. Valtioiden välistä keskustelua tulee tiivistää kybertoimintaympäristöön liittyvissä kysymyksissä niin monenvälisesti, alueellisesti kuin kahdenvälisestikin. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen kyberturvallisuuden kannalta myönteisiä asioita.

2.2 Kybervoima

Kybervoima/valta (engl. Cyber Power) kuvaa valtion kybersuorituskykyä vallankäytön välineinä. Kybervoimaa voidaan käyttää haluttujen tulosten tuottamiseen kyberavaruudessa tai se voi käyttää kyberresursseja tuottamaan haluttuja tuloksia kyberavaruuden ulkopuolella. Kybervoima jakaantuu maailmassa niin eri valtiollisten kuin ei-valtiollisten toimijoiden kesken. Suurvalloille on mahdollista investoida laaja-alaisiin puolustuksellisiin ja hyökkäyksellisiin kyvykkyyksiin, kun taas pienet valtiot keskittyvät erikoisosaamiskykyihin. Useat valtiot kasvattavat maa-, meri- ja ilmavoimiensa rinnalle kybervoimaa ja siihen yhdistyviä kyvykkyyksiä.

Kybertoimintaympäristö on yhä merkittävämpi tila, jossa vaikutetaan Suomen kansalliseen turvallisuuteen. 2020-luvun sodankäyntiin sekoittuu uusia kyberoperaatioelementtejä, joiden tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpitoa voidaan toteuttaa kyberoperaatioiden avulla.

Useat valtiot ja NATO ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin. Kesäkuussa 2021 NATO teki linjauksen, jonka mukaan merkittävät haitalliset kybertoimet voidaan jatkossa tietyissä tapauksissa rinnastaa aseelliseen hyökkäykseen. Lokakuussa 2021 NATO-maiden puolustusministerit sopivat yleissuunnitelmasta, jossa varaudutaan Venäjän mahdolliseen aggressioon, jossa kyberoperaatiot olisivat yksi toimintamuoto.

Kyberkyvykkyyksiä ja niiden käyttöä määritellään eri tavoin, joten yhtenäistä viitekehystä ei ole käytössä. Harvardin Kennedy Schoolin Belfer Centerin kehittämä kansallinen kybervoimaindeksi (NCPI) mittaa valtion kyberkyvykkyyttä seitsemällä eri indikaattoreilla:

1. Kansallinen kyberympäristön valvontakyky,
2. Kansallinen kyberpuolustuskyky ja resilienssi,
3. Informaatioympäristön hallintakyky,
4. Laaja-alainen kybertiedustelukyky,
5. Kansallisen kyberteollisuuden suorituskyky,
6. Kyberhyökkäyskyky,
7. Kyberalan normien ja standardien määrittelykyky.

Ukrainan sota on lisännyt uhkia kyber- ja informaatioympäristössä. Suomen kansallista kybervoimaa/valtaa tulee kehittää edelleen, jota tarvetta mahdollinen NATO-jäsenyys edelleen vahvistaa.

Selonteon näkemys siitä, että kyberhyökkäykset ovat osa Venäjän hyökkäystä Ukrainaan ja että Venäjä todennäköisesti laajentaa kyber- ja informaatio-operaatioitaan Ukrainasta länteen, on erittäin todennäköinen.

3. YHTEISKUNNALLINEN ULOTTUVUUS

Yhteiskuntaan kohdistuvan kyberuhan kohteista keskeisiä ovat kansallisen turvallisuuden kohteet sekä yhteiskunnan elintärkeät toiminnot, joilla turvataan kansalaisten elinmahdollisuudet. Kriittinen infrastruktuuri käsittää ne rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan jatkuvalle toiminnalle. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja. Nämä verkostot eivät ole erillisiä entiteettejä vaan muodostava kansallisen kriittisen

infrastruktuuriverkoston, jossa on paljon keskinäisriippuvuuksia. Yhden systeemin lamaantuminen tai romahtaminen vaikuttaa verkoston muihin osiin.

Selonteko on oikein todennut, että ”Ukrainan tilanne on korostanut entisestään toimitusketjujen hallinnan merkitystä myös ohjelmistojen ja digitaalisten palveluiden osalta.”

Sotaa alempitasoisemman konfliktin yhteydessä valtiollinen toimija tai tämän tukema ja/tai suojaama ryhmittymä voi kohdistaa kyberhyökkäyksiä toista valtiota vastaan ilman, että valtiot olisivat sodassa keskenään. Näille hyökkäyksille on tavanomaista, että tekijät pyrkivät pysymään tuntemattomina ja että valtiot kykenevät kiistämään osallisuutensa niihin.

NATO-prosessin aikana Venäjä voi kohdistaa toimia maamme kriittistä infrastruktuuria kohtaan aiheuttaakseen epävarmuutta ja epäluottamusta kansalaisissa sekä osoittaakseen valtiojohdolle kyvykkyytensä lamauttaa kriittisiä toimintoja.

4. SOTILAALLINEN ULOTTUVUUS

Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta ja kybervoiman käyttöä. Puolustusvoimat varautuu laaja-alaiseen vaikuttamiseen ja kyberpuolustukseen osana kokonaisturvallisuuden mallia. Puolustusselonteon mukaan ”Kyberpuolustusta kehitetään niin, että sen avulla voidaan turvata paremmin paitsi Puolustusvoimien omat myös muut puolustuskykyyn suoraan vaikuttavat järjestelmät.”

Useat valtiot kehittävät kykyään suorittaa operaatioita kyberavaruudessa maan, meren, ilman ja avaruuden lisäksi osana sotilaallista voimankäyttöä. Sotilaallinen suorituskyky perustuu suojaamiseen, tiedusteluun ja vaikuttamiseen.

Kybersodankäynnin strategisen tason kyberoperaatioissa valtio pyrkii vaikuttamaan toisen valtion toimintaan sekä toimintakykyyn. Operatiivisella ja taktisella tasolla kyberoperaatioita suoritetaan osana muuta sotilaallista voimankäyttöä. Tavoitteena voi esimerkiksi olla sotilaallisen johtamisen häiritseminen, lamauttaminen tai harhauttaminen tai sotilaallisen voimankäytön estäminen tai viivästyttäminen.

NATO vahvistanut omaa kyberpuolustuskyvykkyyttään. Kyberpuolustus on osa NATO:n ydintehtävää, kollektiivista puolustusta. NATO:n pääpaino kyberpuolustuksessa on suojella sen omia verkkoja, kyky toimia kyberavaruudessa eri operaatioissa, auttaa liittolaisia vahvistamaan kansallista kyberpuolustuskykyä ja tarjota foorumi poliittiselle konsultaatiolle ja yhteistoiminnalle. NATO:n lähtökohta on, että kukin maa vastaa omasta kyberpuolustuksestaan. Keskeistä on tiedonvaihto, koulutus- ja harjoitustoiminta.

NATO:n jäsenmaat sopivat kesäkuussa 2021 uudesta kyberpuolustuspolitiikasta. Sen mukaan ”merkittävän haitallisen kumulatiivisen kybertoiminnan vaikutusta voidaan tietyissä olosuhteissa pitää aseellisena hyökkäyksenä", tiedonannossa sanotaan.

Kansallisella kyberpuolustuskyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja myös yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Mahdollinen NATO-jäsenyys lisää mahdollisuutta kehittää kansallista suorituskykyämme ja samalla se velvoittaa meitä huolehtimaan tehokkaasti omasta kyberpuolustuksestamme.

Puolustusvoimien kybersuorituskyky suojaamisen, tiedustelun ja vaikuttamisen osalta tulee mitoittaa sellaiseksi, että se mahdollisimman tehokkaasti tukee Puolustusvoimien kokonaissuorituskykyä.

5. TARVITTAVIA TOIMENPITEITÄ SOTILAALLISESSA JA POLIITTISESSA ULOTTUVUUDESSA

5.1 Kansallinen kybertila/kybertoimintaympäristö tulee määritellä

Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen.

Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa. Suomen alueellisen koskemattomuuden valvonta määriteltyyn toimintaympäristöön. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä alueloukkauksen estämiseksi tai torjumiseksi, jotka ovat sidottu lain määrittämään toimintaympäristöön.

Kybertoimintaympäristön vahvistuminen osaksi kansallista toimintaympäristöä tulee aluevalvontalakia ja siihen liittyviä säädöksiä on tarkistettava vastaamaan Suomen kybertoimintaympäristön suojaamisen tarpeita. Uudistus tarvitaan, koska meiltä puuttuu selkeä ja tarkkarajainen juridinen määrittely kansallisesta kybertoimintaympäristöstä. Mahdollinen NATO-jäsenyys vahvistaa tätä tarvetta.

Kansallisen kybertilan määrittely tarvitaan, jotta Suomen kybertilan koskemattomuuden valvonta ja torjunta voidaan tehokkaasti toteuttaa. Tämä tila ei ole vain teknologinen toimintaympäristö vaan merkittävällä tavalla ulko- ja turvallisuuspoliittinen toimintaympäristö.

5.2 Kriittisen infrastruktuurin vahvistaminen

Selonteko on hyvin kiinnittänyt huomiota varautumisen ja jatkuvuudenhallinnan tehostamiseksi. Tarvitaan sekä välittömiä että pitkä ajan toimenpiteitä. Erityisen huomion kohteena tulee olla infrastruktuurin IT-, OT-, SCADA- ja ICS-osat, sillä niiden avulla ohjataan järjestelmiä ja niihin hyökkääjä kohdistaa lamauttavia ja tuhoavia kyberhyökkäyksiä.

Julkisten tietojen mukaan Yhdysvallat ryhtyi auttamaan Ukrainan kriittisen infrastruktuurin suojaamisessa jo viime syksystä alkaen. Todennäköisesti tuon avun turvin Ukrainan kriittisen infrastruktuurin järjestelmiä voitiin puhdistaa ja koventaa.

Meillä voitaisiin käyttää kotimaista kyberturvallisuusosaamista nopeaan järjestelmien suojauksen tehostamiseen. Tätä osaamista on saatavissa alan yrityksistä ja oppilaitoksista.

Pidemmän aikavälin osalta tarvitaan resurssointeja julkisten järjestelmien kyberturvallisuuden parantamiseen ja vahvistamiseen. Lisäksi resursseja tarvitaan kansallisen osaamisen vahvistamiseen.

Selonteko korostaa oikein kybervarautumisen välttämättömyyttä ja jatkuvuuden hallinnan tehostamista. Lisäksi tulee häiriötilanteiden hallintaa parantaa.

5.3 Kansallisen kyberturvallisuuden johtamisen ja tilannetietoisuuden vahvistaminen

Selonteko on tunnistanut tarpeen vahvistaa kyberturvallisuuden johtamista ja tilannetietoisuutta. On aivan välttämätöntä, että Suomella on ajantasaisen kybertilannekuvan lisäksi selkeät johtamis- ja vastuusuhteet, ja toimivaltuudet sekä kyvykkyys hyödyntää kaikkia yhteiskunnan voimavaroja.

Käynnissä oleva NATO-prosessi edellyttää, että kyber/hybriditilannekuvamme ja häiriötilanteiden hallinnan johtamismalli on kunnossa. Vastuut ja toimivaltuudet tulee selkeät ja kaikkien tiedossa. Suomen NATO-prosessi aiheuttaa hyvin todennäköisesti vakavia toimenpiteitä Venäjän taholta.

Siksi tässä vaiheessa olisi perusteltua organisoida operatiivinen kyber/hybridinyrkki Valtioneuvoston kansliaan varmistamaan odotettavissa olevien häiriötilanteiden hallinta. Nyrkkiin voidaan koota maan huippuosaajat yrityksistä ja julkisesta hallinnosta.

Tämän kriisiryhmän tehtävä olisi kartoittaa Suomeen kohdistuvat kyber/hybridiuhat ja haavoittuvuudet, vahvistaa tilannekuvan muodostamista ja ehdottaa tarvittavia toimenpiteitä sekä tukea häiriötilanteiden hallintaa.

Yhteiskunnan digitalisaation lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti. Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta.

6. YHTEENVETO

NATO:n jäsenyys vahvistaisi kansallista kyberturvallisuutta, koska täysjäseninä olisimme oikeutettuja kaikkeen käytettävissä olevaan tietoon, voisimme osallistua puolustussuunnitteluun ja voisimme edelleen vahvistaa kybersuorituskykyämme.

Kansallinen kyberturvallisuus on keskeinen osa kokonaisturvallisuutta, johon meidän on kyettävä osallistamaan eri toimijat sekä yhteensovittamaan voimavarat ja toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi. Kyse on koko yhteiskunnan kyberkyvykkyyden kehittämisestä kriittisen infrastruktuurin suojaamiseksi ja kansalaisten elintärkeiden toimintojen turvaamiseksi.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi